§3.6 模为素数幂的同余式求解

- 观察同余式$x^2 \equiv a \ (mod\ m)$。由定理2.18可知，只需求解$x^2 \equiv a \ (mod\ p^\alpha)$，即可求得$x^2 \equiv a \ (mod\ m)$的所有解。

- 我们已经知道如何求解二次同余式$x^2 \equiv a \ (mod\ p)$，如何由$x^2 \equiv a \ (mod\ p)$的解求$x^2 \equiv a \ (mod\ p^\alpha)$的解？

- 定义3.6.1 设$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_2 x^2 + a_1 x + a_0$，其中$a_i \in Z, i = 0,1, \dots, n$，令
  $$f'(x) = n a_n x^{n-1} + (n-1) a_{n-1} x^{n-2} + \cdots + 2 a_2 x + a_1$$
  称为$f(x)$的导式。

- 定理3.6.1 设$\alpha \geq 2$，且$x \equiv x_1 \ (mod\ p)$是同余式$f(x) \equiv 0 \ (mod\ p)$的一个解，且$(f'(x_1), p) = 1$，令$x_1' \in \{0,1,\dots,p-1\}$且满足$x_1' f'(x_1) \equiv 1 \ (mod\ p)$，

再令

$$x_i = x_{i-1} + t_{i-1}p^{i-1} \left(mod\ p^i\right), i = 2,3,\dots,\alpha$$

其中

$$t_{i-1} = \frac{-f(x_{i-1})}{p^{i-1}} x_1' \ (mod\ p)$$

则同余式$f(x) \equiv 0 \ (mod\ p^\alpha)$有解$x \equiv x_\alpha \ (mod\ p^\alpha)$。

证明：对α用数学归纳法，设$f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_2x^2+a_1x+a_0$。

$(i)\alpha=2$时，因为$x\equiv x_1\ (mod\ p)$是$f(x)\equiv 0\ (mod\ p)$的解，所以$p|f(x_1)$，因此$\frac{f(x_1)}{p}\in Z$，观察同余式$f'(x_1)x\equiv -\frac{f(x_1)}{p}\ (mod\ p)$，因为$(f'(x_1),p)=1$，由定理2.14可知，他有唯一解$x\equiv -\frac{f(x_1)}{p}x_1'=t_1\ (mod\ p)$，

另一方面，我们有$f(x_1+t_1p)=a_n(x_1+t_1p)^n+a_{n-1}(x_1+$

(ii) 设$\alpha-1$时，结论成立，即$x\equiv x_{\alpha-1}\ (mod\ p^{\alpha-1})$是同余式$f(x)\equiv 0\ (mod\ p^{\alpha-1})$的解，所以$p^{\alpha-1}|f(x_{\alpha-1})$，因此$\frac{f(x_{\alpha-1})}{p^{\alpha-1}}\in Z$，观察同余式$f'(x_1)x\equiv -\frac{f(x_{\alpha-1})}{p^{\alpha-1}}\ (mod\ p)$，因为$(f'(x_1),p)=1$，由定理2.14可知，他有唯一解$x\equiv -\frac{f(x_{\alpha-1})}{p^{\alpha-1}}x_1'=t_{\alpha-1}\ (mod\ p)$，又因为$x_i=x_{i-1}+t_{i-1}p^{i-1}\left(mod\ p^i\right),i=2,3,\ldots,\alpha$，所以$x_i\equiv x_{i-1}\ (mod\ p)$，因此$x_{\alpha-1}\equiv x_1\ (mod\ p)$，有$f'(x_{\alpha-1})\equiv f'(x_1)\ (mod\ p)$，所以$x\equiv t_{\alpha-1}\ (mod\ p)$也是同余式$f'(x_{\alpha-1})x\equiv -\frac{f(x_{\alpha-1})}{p^{\alpha-1}}\ (mod\ p)$的唯一解。

另一方面，我们有$f(x_{\alpha-1}+t_{\alpha-1}p^{\alpha-1})=a_n(x_{\alpha-1}+$

- 例3.6.1 求解同余式$f(x) = x^2 + 1 \equiv 0 \ (mod\ 25)$

- 例3.6.1 求解同余式$f(x)=x^2+1\equiv 0\ (mod\ 25)$

解：易知$25=5^2$，$f'(x)=2x$。

首先求解同余式$x^2+1\equiv 0\ (mod\ 5)$，即$x^2\equiv 4\ (mod\ 5)$，显然解为$x\equiv \pm 2\ (mod\ 5)$，对$x_1\equiv 2\ (mod\ 5)$，求得$f'(x_1)=4$，从而$x_1'=4$，因此$t_1=-1\cdot 4\equiv 1\ (mod\ 5)$，进一步求得$x_2=2+1\cdot 5=7\ (mod\ 25)$；

对$x_1\equiv -2\ (mod\ 5)$，类似可得$t_1=-1\cdot 1\equiv -1\ (mod\ 5)$，进一步求得$x_2=-2+(-1)\cdot 5=-7\equiv 18\ (mod\ 25)$。

综上可知，$x\equiv \pm 7\ (mod\ 25)$都是同余式$f(x)=x^2+1\equiv 0\ (mod\ 25)$的解。

- 例3.6.2 求同余式$f(x) = x^4 + 7x + 1 \equiv 0 \ (mod\ 27)$的一个解

- 例3.6.2 求同余式$f(x) = x^4 + 7x + 1 \equiv 0 \ (mod\ 27)$的一个解

解：易知$27 = 3^3$，$f'(x) = 4x^3 + 7$。

首先求得同余式$x^4 + 7x + 1 \equiv 0 \ (mod\ 3)$的一个解$x_1 \equiv 1 \ (mod\ 3)$，此时有$f'(x_1) = 11$，从而$x_1' = 2$，因此$t_1 = -2 \cdot 1 \equiv 1 \ (mod\ 3)$，进一步求得$x_2 = 1 + 1 \cdot 3 = 4 \ (mod\ 9)$；进而有$t_2 = -2 \cdot 2 \equiv 2 \ (mod\ 3)$，进一步求得$x_3 = 4 + 2 \cdot 9 = 22 \ (mod\ 27)$，因此$x \equiv 22 \ (mod\ 27)$是同余式$f(x) = x^4 + 7x + 1 \equiv 0 \ (mod\ 27)$的一个解。

进一步我们有如下定理

- 定理3.6.2 设$\alpha \geq 2$，且同余式$f(x) \equiv 0 \ (mod\ p)$和$f'(x) \equiv 0 \ (mod\ p)$没有公共解，则同余式$f(x) \equiv 0 \ (mod\ p^{\alpha})$和$f(x) \equiv 0 \ (mod\ p)$的解数相等。

证明：仅需证明$f(x)\equiv 0\ (mod\ p^i)$的解和$f(x)\equiv 0\ (mod\ p^{i+1})$存在一一对应的关系，$i=1,2,\ldots$。

事实上，因为$f(x)\equiv 0\ (mod\ p)$和$f'(x)\equiv 0\ (mod\ p)$没有公共解，因此$f(x)\equiv 0\ (mod\ p)$的解x_1不满足$f'(x)\equiv 0\ (mod\ p)$，即$(f'(x_1),p)=1$，由定理3.6.1可知，每一个$f(x)\equiv 0\ (mod\ p^i)$的解$x\equiv x_i\ (mod\ p^i)$都可推出一个$f(x)\equiv 0\ (mod\ p^{i+1})$的解$x\equiv x_{i+1}=x_i+t_ip^i(mod\ p^{i+1})$，因此我们只需证明在模$p^{i+1}$的一个完全剩余系中，不存在另一个由$x\equiv x_i\ (mod\ p^i)$衍生出的$f(x)\equiv 0\ (mod\ p^{i+1})$的解，为此我们仅需证明$x_{i+1}+jp^i, j=1,2,\ldots,p-1$都不是$f(x)\equiv 0\ (mod\ p^{i+1})$的解，

因为$x \equiv x_{i+1} \ (mod\ p^{i+1})$是$f(x) \equiv 0 \ (mod\ p^{i+1})$的解，所以$f(x_{i+1}) \equiv 0 \ (mod\ p^{i+1})$，此时$f\left(x_{i+1} + jp^{i}\right)$=$a_n\left(x_{i+1} +\right.$

- 例3.6.1 求解同余式$f(x) = x^2 + 1 \equiv 0\ (mod\ 25)$

由定理3.6.2可知， $x \equiv \pm 7\ (mod\ 25)$是同余式$f(x) = x^2 + 1 \equiv 0\ (mod\ 25)$的全部解。

§3.7 模m的二次同余式

- 首先我们考虑模数是奇素数幂的情况

- 定理3.7.1 设p是奇素数，则同余式
$$x^2 \equiv a \ (mod\ p^{\alpha}), (a, p) = 1, \alpha \geq 1$$
有解当且仅当a是模p的二次剩余，且此时共有2个解。

证明：($\Longrightarrow$)因为$x^2 \equiv a \ (mod\ p^\alpha)$有解，设$x \equiv x_1 \ (mod\ p^\alpha)$是他的一个解，因此$x_1^2 \equiv a \ (mod\ p^\alpha)$，进而有$x_1^2 \equiv a \ (mod\ p)$，即$x^2 \equiv a \ (mod\ p)$有解，$a$是模$p$的二次剩余。

证明：($\Longrightarrow$)因为$x^2 \equiv a \ (mod\ p^\alpha)$有解，设$x \equiv x_1 \ (mod\ p^\alpha)$是他的一个解，因此$x_1^2 \equiv a \ (mod\ p^\alpha)$，进而有$x_1^2 \equiv a \ (mod\ p)$，即$x^2 \equiv a \ (mod\ p)$有解，$a$是模$p$的二次剩余。

($\Longleftarrow$)因为a是模p的二次剩余，所以同余式$x^2 \equiv a \ (mod\ p)$有解，设$x \equiv x_1 \ (mod\ p)$是他的一个解，显然$x_1 \not\equiv 0 \ (mod\ p)$。令$f(x) = x^2 - a$，则$f'(x) = 2x$，进一步可知$x \equiv x_1 \ (mod\ p)$是$f(x) \equiv 0 \ (mod\ p)$的一个解，且$(f'(x_1), p) = (2x_1, p) = 1$，因此由定理3.6.1可知$f(x) \equiv 0 \ (mod\ p^\alpha)$有解，即$x^2 \equiv a \ (mod\ p^\alpha)$有解。

证明：$(\Longrightarrow)$因为$x^2 \equiv a \ (mod\ p^\alpha)$有解，设$x \equiv x_1 \ (mod\ p^\alpha)$是他的一个解，因此$x_1^2 \equiv a \ (mod\ p^\alpha)$，进而有$x_1^2 \equiv a \ (mod\ p)$，即$x^2 \equiv a \ (mod\ p)$有解，$a$是模$p$的二次剩余。

$(\Longleftarrow)$因为a是模p的二次剩余，所以同余式$x^2 \equiv a \ (mod\ p)$有解，设$x \equiv x_1 \ (mod\ p)$是他的一个解，显然$x_1 \not\equiv 0 \ (mod\ p)$。令$f(x) = x^2 - a$，则$f'(x) = 2x$，进一步可知$x \equiv x_1 \ (mod\ p)$是$f(x) \equiv 0 \ (mod\ p)$的一个解，且$(f'(x_1), p) = (2x_1, p) = 1$，因此由定理3.6.1可知$f(x) \equiv 0 \ (mod\ p^\alpha)$有解，即$x^2 \equiv a \ (mod\ p^\alpha)$有解。

此时，因为对$x^2 \equiv a \ (mod\ p)$的任意解$x \equiv x_1 \ (mod\ p)$，都有$(f'(x_1), p) = (2x_1, p) = 1$，所以$f(x) \equiv 0 \ (mod\ p)$和$f'(x) \equiv 0 \ (mod\ p)$无公共解，由定理3.6.2可知，$x^2 \equiv a \ (mod\ p^\alpha)$和$x^2 \equiv a \ (mod\ p)$的解数相等，而$x^2 \equiv a \ (mod\ p)$显然有2个解，证毕。

- 再考虑模数是2的幂的情况

- 定理3.7.1 设$\alpha > 1$，则同余式

$$x^2 \equiv a \ (mod\ 2^\alpha), (a, 2) = 1, \alpha \geq 1$$

有解的充要条件是

(i) 当$\alpha = 2$时，$a \equiv 1 \ (mod\ 4)$，此时共有2个解;

(ii)当$\alpha \geq 3$时，$a \equiv 1 \ (mod\ 8)$，此时共有4个解。

证明：因为$x^2 \equiv a \ (mod\ 2^\alpha)$有解，设$x \equiv x_1 \ (mod\ 2^\alpha)$是他的一个解，因此$x_1^2 \equiv a \ (mod\ 2^\alpha)$，由于$(a, 2) = 1$，所以$(x_1, 2) = 1$，设$x_1 = 1 + 2t, t \in Z$，此时有$a \equiv x_1^2 = 1 + 4t(t+1) \ (mod\ 2^\alpha)$，

(i)当$\alpha = 2$时，$a \equiv 1 + 4t(t+1) \equiv 1 \ (mod\ 4)$，必要性得证。此时，易知$x \equiv \pm 1 \ (mod\ 4)$是同余式$x^2 \equiv a \equiv 1 \ (mod\ 4)$的全部解，充分性得证，且共有2个解；

(ii) 当$\alpha \geq 3$时，显然有$8|2^\alpha$，且$2|t(t+1)$，因此由$a \equiv 1 + 4t(t+1) \ (mod\ 2^\alpha)$可知$a \equiv 1 + 4t(t+1) \equiv 1 \ (mod\ 8)$，必要性得证。

接下来用数学归纳法证明充分性，此时有$a \equiv 1\ (mod\ 8)$，

(a)当$\alpha = 3$时，易知$x \equiv \pm 1, \pm 3\ (mod\ 8)$是同余式$x^2 \equiv a \equiv 1\ (mod\ 8)$的全部解，充分性得证，且共有4个解；

(b)设$\alpha - 1 (\geq 3)$时，$x^2 \equiv a\ (mod\ 2^{\alpha-1})$有解，令$x \equiv x_1\ (mod\ 2^{\alpha-1})$是他的一个解，因此$x_1^2 \equiv a\ (mod\ 2^{\alpha-1})$，由于$(a, 2) = 1$，所以$(x_1, 2) = 1$，即$x_1$是奇数，令$b = \frac{a - x_1^2}{2^{\alpha-1}} \in Z$，则$(x_1 + 2^{\alpha-2}b)^2 = x_1^2 + 2^{\alpha-1}x_1 b + 2^{2(\alpha-2)}b^2 \equiv x_1^2 + 2^{\alpha-1}b = a\ (mod\ 2^{\alpha})$，因此$x \equiv x_1 + 2^{\alpha-2}b (mod\ 2^{\alpha})$是$x^2 \equiv a\ (mod\ 2^{\alpha})$的一个解，充分性得证。

此时，设$x \equiv x_2\ (mod\ 2^\alpha)$是$x^2 \equiv a\ (mod\ 2^\alpha)$的一个解，则显然有$(x_2 + 2^{\alpha-1})^2 = x_2^2 + 2^\alpha x_2 + 2^{2(\alpha-1)} \equiv x_2^2 \equiv a\ (mod\ 2^\alpha)$，因此$x \equiv \pm x_2, \pm x_2 + 2^{\alpha-1} (mod\ 2^\alpha)$是$x^2 \equiv a\ (mod\ 2^\alpha)$的4个解，任取$x^2 \equiv a\ (mod\ 2^\alpha)$的一个解$x \equiv x_3\ (mod\ 2^\alpha)$，因为$x_2^2 \equiv a \equiv x_3^2 (mod\ 2^\alpha)$，故$(x_2 - x_3)(x_2 + x_3) \equiv 0\ (mod\ 2^\alpha)$，又显然$x_2, x_3$都是奇数，所以$x_2 - x_3, x_2 + x_3$都是偶数，所以$\frac{x_2-x_3}{2} \cdot \frac{x_2+x_3}{2} \equiv 0\ (mod\ 2^{\alpha-2})$，仍因$x_2, x_3$都是奇数$\frac{x_2-x_3}{2}, \frac{x_2+x_3}{2}$必为1奇1偶，因此

$(a)\ \frac{x_2-x_3}{2} \equiv 0\ (mod\ 2^{\alpha-2})$，有$x_2 - x_3 \equiv 0\ (mod\ 2^{\alpha-1})$，此时$x_3 \equiv x_2$或$x_2 + 2^{\alpha-1} (mod\ 2^\alpha)$；

$(b) \frac{x_2+x_3}{2} \equiv 0\ (mod\ 2^{\alpha-2})$，有$x_2 + x_3 \equiv 0\ (mod\ 2^{\alpha-1})$，此时$x_3 \equiv -x_2$或$-x_2 + 2^{\alpha-1} (mod\ 2^\alpha)$。

综上可知，共有4个解，证毕。

- 例3.7.1 求解同余式$x^2 \equiv 9 \ (mod\ 16)$

- 例3.7.1 求解同余式$x^2 \equiv 9 \ (mod\ 16)$

解：显然$x \equiv 3 \ (mod\ 16)$是同余式$x^2 \equiv 9 \ (mod\ 16)$的一个解，因此共有4个解：$x \equiv \pm 3, \pm 11 \ (mod\ 16)$。

- 例3.7.2 求解同余式$x^2 \equiv 17\ (mod\ 32)$

- 例3.7.2 求解同余式$x^2 \equiv 17\ (mod\ 32)$

解：先求同余式$x^2 \equiv 17\ (mod\ 16)$的一个解，显然$x \equiv 1\ (mod\ 16)$是需要的解，由此构造$x^2 \equiv 17\ (mod\ 32)$的一个解：令$b = \frac{a - x_1^2}{2^{\alpha-1}} = \frac{17-1}{16} = 1$，则$x \equiv x_1 + 2^{\alpha-2} b (mod\ 2^{\alpha})$即$x \equiv 1 + 2^3 \cdot 1 \equiv 9 (mod\ 2^5)$是$x^2 \equiv 17\ (mod\ 32)$的一个解，因此4个解为$x \equiv \pm 9, \pm 25\ (mod\ 32)$。

§3.8 表素数为平方和

- 定理3.8.1 设p是素数，则方程

$$x^2 + y^2 = p$$

有整数解的充要条件是$p = 2$或$p \equiv 1\ (mod\ 4)$

证明：($\Longrightarrow$)因为$x^2+y^2=p$有整数解，设(x_0,y_0)是一组整数解，则有$x_0^2+y_0^2=p$且$0<|x_0|,|y_0|<p$，因此$(x_0,p)=(y_0,p)=1$，进而存在$y_0'\in Z$，使得$y_0y_0'\equiv 1\ (mod\ p)$，当$p\neq 2$即$p$是奇素数时，$(x_0y_0')^2=(p-y_0^2)(y_0')^2\equiv -(y_0y_0')^2\equiv -1\ (mod\ p)$，所以$-1$是模$p$的二次剩余，因此$p\equiv 1\ (\ mod\ 4)$。

($\Longleftarrow$)当$p=2$，显然有$1^2+1^2=2$，方程有解；

若$p\neq 2$，则$p\equiv 1\ (\ mod\ 4)$，有$\left(\frac{-1}{p}\right)=1$，所以存在$x_0\in Z, 0<|x_0|<\frac{p}{2}$，使得$x_0^2\equiv -1\ (mod\ p)$，令$y_0=1$，则有$x_0^2+y_0^2\equiv 0\ (mod\ p)$，因此存在正整数$m_0$，使得$x_0^2+y_0^2=m_0p$，设$m$是使方程$x^2+y^2=mp$有整数解的最小正整数$m$，

若$m>1$，从模m的绝对值最小完全剩余系中取两个整数u,v，使得$u\equiv x_0, v\equiv y_0\ (mod\ m)$，则有$|u|,|v|\le\frac{m}{2}$，此时有$0<u^2+v^2\le\frac{m^2}{2}, u^2+v^2\equiv x_0^2+y_0^2\equiv 0\ (mod\ m)$，因此存在$m'\in Z$，使得$u^2+v^2=m'm$，此时有$m'pm^2=(u^2+v^2)(x_0^2+y_0^2)=(ux_0+vy_0)^2+(uy_0-vx_0)^2$，因为$ux_0+vy_0\equiv x_0^2+y_0^2\equiv 0\ (mod\ m), uy_0-vx_0\equiv x_0y_0-y_0x_0=0\ (mod\ m)$，令$x_1=\frac{ux_0+vy_0}{m}, y_1=\frac{uy_0-vx_0}{m}$，则$x_1,y_1\in Z$，又因为$m'm=u^2+v^2\le\frac{m^2}{2}$，所以$m'\le\frac{m}{2}<m$，因此$x_1^2+y_1^2=m'p$，与$m$的最小性矛盾，所以$m=1$，即方程$x^2+y^2=p$有解，证毕。

- 例3.8.1 已知$p = 797$是素数，求正整数x, y，使得$x^2 + y^2 = p$

解：因为$797 \equiv -3\ (mod\ 8)$，所以$\left(\frac{2}{797}\right) = -1$，因此

$2^{\frac{797-1}{2}} \equiv -1\ (mod\ 797)$，即$(2^{\frac{797-1}{4}})^2 \equiv -1\ (mod\ 797)$，所以$x_0 = 2^{\frac{797-1}{4}} \equiv 2^{199} \equiv 215\ (mod\ 797)$是$x^2 \equiv -1$的一个解，

令$y_0 = 1$，则$m_0 = \frac{x_0^2+y_0^2}{p} = 58$，

令$u_0 \equiv x_0 \equiv -17 (mod\ m_0), v_0 \equiv y_0 \equiv 1\ (mod\ m_0), x_1 = \frac{u_0x_0+v_0y_0}{m_0} = -63, y_1 = \frac{u_0y_0-v_0x_0}{m_0} = -4$，则$m_1 = \frac{x_1^2+y_1^2}{p} = 5$，

再令$u_1 \equiv x_1 \equiv 2 (mod\ m_1), v_1 \equiv y_1 \equiv 1\ (mod\ m_1), x_2 = \frac{u_1x_1+v_1y_1}{m_1} = -26, y_2 = \frac{u_1y_1-v_1x_1}{m_1} = 11$，则$m_2 = \frac{x_2^2+y_2^2}{p} =1$，

因此$x = 26, y = 11$是$x^2 + y^2 = p$的解。

- 用二次剩余设计的密码方案I（Rabin方案的Williams改进）
  - 设p,q是形如$4k+3$的大素数，$n=pq$，则公钥为n，私钥为(p,q)。
  - 消息m满足$0<m<\frac{n}{2},\left(\frac{m}{n}\right)=1$，则$c=E(m)=m^2\ (mod\ n)$
  - 解密时，求解同余式组

$$\begin{cases} x^2 \equiv c\ (mod\ p) \\ x^2 \equiv c\ (mod\ q) \end{cases}$$

可得4个解，其中仅有一个m'满足$0<m'<\frac{n}{2},\left(\frac{m'}{n}\right)=1$，则$m'=D(c)$。

- 方案的正确性

证明：由于c是模n的二次剩余，因此同余式组

$$\begin{cases} x^2 \equiv c \ (mod\ p) \\ x^2 \equiv c \ (mod\ q) \end{cases}$$

有4个解，事实上有$\begin{cases} x \equiv \pm m \ (mod\ p) \\ x \equiv \pm m \ (mod\ q) \end{cases}$，因此4个解分别为

$x = m, n - m, q'qm_p - p'pm_q \ (mod\ n), n - \big(q'qm_p -$

又因为$\left(\frac{m}{n}\right) = 1$，所以有$\left(\frac{q'qm_p - p'pm_q \ (mod\ n)}{n}\right) = \left(\frac{q'qm_p - p'pm_q}{n}\right) = \left(\frac{q'qm_p - p'pm_q}{p}\right)\left(\frac{q'qm_p - p'pm_q}{q}\right) = \left(\frac{m_p}{p}\right)\left(\frac{-m_q}{q}\right) = \left(\frac{-1}{q}\right)\left(\frac{m}{p}\right)\left(\frac{m}{q}\right) = \left(\frac{-1}{q}\right)\left(\frac{m}{n}\right) = \left(\frac{-1}{q}\right)$，类似的有$\left(\frac{n - (q'qm_p - p'pm_q)(mod\ n)}{n}\right) = \left(\frac{-1}{p}\right)$，但是我们有$p, q \equiv 3\ (mod\ 4)$，因此$\left(\frac{-1}{q}\right) = \left(\frac{-1}{p}\right) = -1$，故4个解中仅有一个满足$0 < x < \frac{n}{2}, \left(\frac{x}{n}\right) = 1$，即为明文$m$。

注：我们注意到c是模n的二次剩余，因此它既是模p的二次剩余，也是模q的二次剩余，因此$\left(\frac{c}{p}\right)=c^{\frac{p-1}{2}}\equiv 1\ (mod\ p),\left(\frac{c}{q}\right)=c^{\frac{q-1}{2}}\equiv 1\ (mod\ q)$，此时有$c^{\frac{p+1}{2}}\equiv c\ (mod\ p)$，$c^{\frac{q+1}{2}}\equiv c\ (mod\ q)$，又因为$p,q\equiv 3\ (mod\ 4)$，所以$4|p+1,4|q+1$，因此同余式$x^2\equiv c\ (mod\ p)$的解为$\pm c^{\frac{p+1}{4}}\ (mod\ p)$，$x^2\equiv c\ (mod\ q)$的解为$\pm c^{\frac{q+1}{4}}\ (mod\ q)$，再由孙子定理可求得同余式$x^2\equiv c\ (mod\ n)$的4个解，由上述证明可知其中有且仅有一个满足$0<x<\frac{n}{2},\left(\frac{x}{n}\right)=1$，即为明文$m$。

- 用二次剩余设计的密码方案II（Goldwasser-Micali方案）
  - 设p, q是大素数，$n = pq$，令x满足$\left(\frac{x}{p}\right) = \left(\frac{x}{q}\right) = -1$，则公钥为$(n, x)$，私钥为$(p, q)$。
  - 消息m为一个比特，随机取$y, (y, n) = 1$，则$c = E(m) = y^2 x^m \ (mod\ n)$
  - 解密时，求$\left(\frac{c}{p}\right)$和$\left(\frac{c}{q}\right)$，如果$\left(\frac{c}{p}\right) = \left(\frac{c}{q}\right) = 1$，则$m' = D(c) = 0$，否则$m' = D(c) = 1$。

- 方案的正确性

证明：显然如果$m = 0$，则$E(m)$为模n的二次剩余；如果$m = 1$，则$E(m)$为模n的二次非剩余。因此解密时，仅需判断c是否为模n的二次剩余，因为同余式$x^2 \equiv c \ (mod\ n)$和同余式组

$\begin{cases} x^2 \equiv c \ (mod\ p) \\ x^2 \equiv c \ (mod\ q) \end{cases}$的解相同，因此$c$为模$n$的二次剩余当且仅当

$\left(\frac{c}{p}\right) = \left(\frac{c}{q}\right) = 1$，此时$m = 0$，正确性得证。

- 方案的正确性

证明：显然如果$m = 0$，则$E(m)$为模n的二次剩余；如果$m = 1$，则$E(m)$为模n的二次非剩余。因此解密时，仅需判断c是否为模n的二次剩余，因为同余式$x^2 \equiv c \ (mod\ n)$和同余式组$\begin{cases} x^2 \equiv c \ (mod\ p) \\ x^2 \equiv c \ (mod\ q) \end{cases}$的解相同，因此$c$为模$n$的二次剩余当且仅当$\left(\frac{c}{p}\right) = \left(\frac{c}{q}\right) = 1$，此时$m = 0$，正确性得证。

- 方案的安全性依赖于判断一个随机数是否为模n的二次剩余这一问题。

上机练习

- 用二次剩余设计的密码方案II（Goldwasser-Micali方案）
  - 取$p = 613, q = 827$都是10位的素数，$n = pq = 506951$，令x满足$\left(\frac{x}{p}\right) = \left(\frac{x}{q}\right) = -1$，则公钥为$n, x$，私钥为$p, q$。
  - 消息m为一个比特，随机取$y, (y, n) = 1$，则$c = E(m) = y^2 x^m \ (mod\ n)$
  - 解密时，求$\left(\frac{c}{p}\right)$和$\left(\frac{c}{q}\right)$，如果$\left(\frac{c}{p}\right) = \left(\frac{c}{q}\right) = 1$，则$m' = D(c) = 0$，否则$m' = D(c) = 1$。
- 要求输出中间结果，包括$x, y, c, \left(\frac{c}{p}\right), \left(\frac{c}{q}\right), m'$

上机练习

- 作业：实现算法3.1（模p平方根算法）并计算同余式$x^2 \equiv 315\ (mod\ 907)$的所有解。

- 要求输出所有中间结果和最终结果。